



CVE-2012-6123

Published on: 10/31/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:22 PM UTC

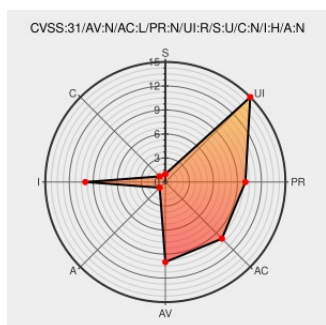
CVE-2012-6123

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Chicken](#) from [Call-cc](#) contain the following vulnerability:

Chicken before 4.8.0 does not properly handle NUL bytes in certain strings, which allows an attacker to conduct "poisoned NUL byte attack."

CVE-2012-6123 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **chicken** - **chicken** version **before 4.8.0**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Broken Link access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2012-6123

NO vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)